

SECRET

Central Intelligence Agency

DD/A Registry

82-0538/105



Washington, D.C. 20505

25 SEP 1982

MEMORANDUM FOR: House Permanent Select Committee for Intelligence
Senate Select Committee for Intelligence

SUBJECT: Report on the SAFE Project

REFERENCE: Intelligence Authorization Act for FY-83

1. The attached report on the SAFE Project is in response to the request contained in the reference. I have reviewed and approved the report and it has been coordinated with DIA.

2. The report describes the redirected SAFE development program and how it will be implemented. It includes total system cost, schedule, and capability milestones for each agency.

3. I believe the redirection provides the most manageable, cost effective, and least-risk approach to satisfying intelligence production requirements in both CIA and DIA. I appreciate and support the committee's stated belief that the SAFE Project is vitally important to the Intelligence Community and that the joint development effort must continue.

/s/ John N. McMahon

John N. McMahon
Acting Director of Central Intelligence

Attachment

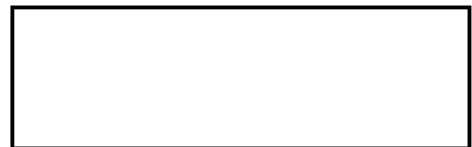


Regraded Unclassified When
Separated From Attachment

SECRET

SECRET

PROJECT SAFE
REPORT TO CONGRESS
23 September 1982



25X1

SECRET

SECRET

EXECUTIVE SUMMARY

The Preliminary Design Review (PDR) for the initial CIA SAFE delivery was held from November 1981 through January 1982. Serious questions surfaced concerning management, technical development, cost and schedule. Subsequently the DDCI and DD/DIA directed an audit of the SAFE program be performed. The Audit Report was completed in April 1982 and briefed to the DDCI and DD/DIA along with the SAFE Steering Committee.

The Audit findings indicated ineffective management, serious flaws in the technical approach, a program that would slip a minimum of 18 months from projected schedules (late 83 for CIA; late 84 for DIA), and a probable cost growth to \$200 million at completion. Indeed, the audit findings seriously questioned whether SAFE could have been successfully completed using the initial development approach. After the Audit results were presented to the Agencies, the Consolidated SAFE Project Office (CSP0) was directed to develop options that were responsive to the Audit findings.

In June 1982, the CSP0 presented two basic options. First, the software development approach which capitalized on the work already performed in the Burroughs environment and second, a software integration approach which capitalized on commercially available software packages operating in an IBM compatible environment. The CSP0 recommended the software integration approach, accepting the risk in software integration vice major software development.

The DCI and the Director of DIA concurred in the recommendation to build SAFE using commercially available off-the-shelf software packages to satisfy SAFE requirements to the maximum extent possible. Augmentations or enhancements would be evaluated on a case by case basis and incorporated only after thorough review by the respective agencies. The software packages would be integrated into an IBM compatible environment. An early capability would be provided to both agencies, in the spring of 1983, using operational software already available in the CIA. In response to criticisms of the project management, the new program manager has directed the following:

1. The SAFE development facility will be moved from the West Coast to the East Coast as soon as practical (the move is planned for 1983).
2. A strong Quality Assurance and Validation/Verification function will be provided by the CSP0 with assistance from an independent contractor.

3. TRW's role to be significantly reduced as result of the redirection. Their staff was cut back from 320 in late 1981 to 79 currently.

4. The hardware will be provided by the government vice handled through TRW.

5. The development of an encrypted Wideband Bus Communications System to be discontinued. Escalating development costs resulted in a determination that the cost could not be justified based on the capability that would be delivered against the current SAFE requirement set. The discontinuance resulted in a projected cost avoidance [REDACTED]

25X1

25X1

Current CSPO and TRW efforts (to be completed in October 1982) are involved in evaluation of available software packages. The next phase, October 1982 to System Design Review (SDR) in February 1983, will be devoted to planning and designing the integration and augmentation (where necessary) of the SAFE system. In addition to the early capabilities being provided in 1983, enhancements to the early capabilities are planned for both agencies in 1984 and Integrated SAFE deliveries for both agencies.

25X1

SECRET

	Page
I. PREFACE	4
A. PURPOSE	
B. REPORT ORGANIZATION	
II. BACKGROUND	5
A. CHRONOLOGY	
B. SAFE REQUIREMENTS	
C. SAFE AUDIT FINDINGS	
III. SAFE OPTIONS CONSIDERED	10
A. METHODOLOGY IN EVALUATION PROCESS	
B. RESULTS AND CONCLUSIONS	
1. SOFTWARE DEVELOPMENT APPROACH	
2. SOFTWARE INTEGRATION APPROACH	
3. RISK ASSESSMENT OF APPROACHES	
C. COMMUNICATIONS OPTIONS	
IV. MANAGEMENT APPROACH FOR REDIRECTION OF SAFE	20
A. INTRODUCTION AND CSPO EVALUATION	
B. LINE MANAGEMENT OVERSIGHT AND COORDINATION	
C. ORGANIZATION	
1. QUALITY ASSURANCE	
2. SYSTEM DEVELOPMENT	
3. OPERATIONAL SUPPORT	
D. INTEGRATION	
E. SOFTWARE MANAGEMENT	
F. DEVELOPMENT CONTRACTOR	
V. SOFTWARE PACKAGE SELECTION AND EVALUATION (TASKS AND STATUS)	26
A. INTRODUCTION	
B. DBMS STUDY	
C. OTHER SOFTWARE PACKAGE STUDY	
D. USER LANGUAGE	
E. REQUIREMENTS CLOSURE	
F. CONVERSION ANALYSIS	
G. SYSTEM ENGINEERING ANALYSIS	
VI. SCHEDULE	39
VII. COST	42

SECRET

I. PREFACE

A. PURPOSE

The purpose of this report is to describe actions directed by the DCI and Director, DIA in conjunction with the Consolidated SAFE Project Office (CSPO). The report covers a brief summary of the findings of the SAFE Audit Team and a redirection approach which addresses the concerns identified in the SAFE Audit Report dated 1 April 1982. Because the redirection assumes the original SAFE requirements continue to be valid, the report contains a brief summary statement of those requirements.

B. REPORT ORGANIZATION

This report is divided into seven sections, including the Preface (Section I). Section II provides a chronology and restates the functional requirements for the CIA and DIA which were used as a basis of estimate by the CSPO study teams in developing options and recommendations. In addition, Section II also summarizes the findings of the SAFE Audit. Section III documents the procedures followed by CSPO in developing the options in response to the audit results. Section IV presents the new approach to SAFE management. Section V is a summary and status of the software package evaluation currently underway (to be completed in October 1982). Section VI outlines the schedule and Section VII covers cost.

II. BACKGROUND

A. CHRONOLOGY

During the past year, concerns were expressed by the CSPO that major deficiencies existed in the software design for the SAFE System. A Preliminary Design Review (PDR) for SAFE was held during the period November 1981 through January 1982. This PDR provided to the government documentation with which to measure how well the SAFE System Design met the requirements. As a result of this review, the government determined that significant design issues were unresolved and could adversely impact the project cost and schedule. Based upon this evaluation, an Audit was directed by the DDCI and the DD/DIA to examine the SAFE Program in its entirety. The audit findings were provided to the DDCI and the DD/DIA along with the SAFE Steering Committee in April 1982. Subsequent to their review, the CSPO was tasked to develop alternatives which were responsive to the Audit findings. These alternatives were briefed to the DCI in June and July 1982 and also to the Director, DIA in July 1982.

B. SAFE REQUIREMENTS

The objective of the SAFE system is to improve the quality and timeliness of U. S. Intelligence. Precedence over the past few years has been given to providing more coverage, increased capacity and greater sophistication to our information collection capability. We have been so successful that in many instances we have inundated the intelligence analyst with information. The purpose of SAFE is to provide the needed data processing support to assist the analyst in coping with the myriad sources and large quantities of data available on a given subject. SAFE will relieve the analyst from the time-consuming tasks of collecting, organizing, collating, editing and coordinating these data in order to provide more time to analyze the data for significance and to provide more meaningful, accurate and timely reports to the decision makers.

Specifically, SAFE will provide support to the analyst in the following key areas:

- the flow of information to and from the analyst,
- the improved efficiency and simplicity in the analyst work environment,
- the maintenance of currency and accuracy of large data base holdings and,
- the production of finished intelligence reports:

SECRET

To significantly improve the flow of intelligence data, SAFE will provide automatic message processing and dissemination of incoming electrical traffic. This will allow analysts to develop interest profiles which serve to quickly direct relevant traffic to individuals in accordance with their responsibilities. These user profiles may also be structured to alert the analyst when specific intelligence data of topical sensitivity is received by the respective agency (CIA/DIA).

In addition to accelerating the dissemination of electrical traffic, SAFE will provide the capability for a user to read, add comments, route (to other analysts, to other branches, etc.) and index intelligence items. This allows analysts to better communicate with one another on items of current intelligence and is especially useful during a crisis situation.

Work files are another capability provided by SAFE. Work files are central to SAFE's concept of allowing the analyst the means to exploit system resources to satisfy unique, individual needs. Work files can be defined and structured to meet individual data storage and retrieval requirements. The user can define output formats so that data presentation at the workstation terminal focuses attention on relevant information.

More effective exploitation of collection resources will be another benefit from SAFE. Timely dissemination of intelligence data to the analyst will serve to facilitate communication and coordination between the manager of collection resources and the intelligence analyst. In SAFE, the evaluation process associated with collection management will be automated with results available quickly and on-line, thus providing a more effective exploitation of our collection resources.

A major improvement to the analyst environment provided by SAFE is the provision for a single access language to the several personal and shared data bases. This capability supports the current intelligence function as well as historical research. On-line access to reference data will allow the SAFE user to search not only indexed records on order of battle or installations of intelligence interest, but also to search abstracts of documents and full text electrical messages, all through a single user language. This SAFE feature will support rapid query and file maintenance across diverse data bases with the confidence that all relevant and accurate data can be brought to bear on a particular intelligence problem or question.

The SAFE User Language has been defined based on a model of the intelligence analyst's work environment. Thus, the user-interface is structured to allow the user to perform multiple functions simultaneously, improving analytical efficiency and allowing greater attention to be paid to the analysis function by the analyst and less attention to support tasks which are accomplished by the SAFE system.

SECRET

Many existing DIA data bases contain data duplication, and lack data standardization and data integrity. The objective of SAFE is to integrate data bases where feasible in an effort to optimize data base maintenance and retrieval while at the same time reducing the risk of data inconsistency. The ability to perform on-line maintenance in a timely manner while reducing data duplication will enhance the probability that the consumer of the intelligence product will be provided consistent, timely, and comprehensive intelligence estimates and appraisals.

Finally, SAFE will significantly improve the mechanism for producing finished intelligence. This is a particularly important aspect to the Department of Defense Intelligence Information System (DODIIS) community for contingency planning and strategic targeting. In addition to providing the mechanism to provide for a more accurate and timely data base update, SAFE also affords the user the capability to write, route for review, and print finished intelligence reports. The provision for on-line text composition allows the user to write memoranda, articles, reports, and then to print the textual or structured data in a variety of output formats. Because of the integrated nature of the SAFE user-interface, data resident in structured production data bases can also be easily moved and copied into these work files supporting the finished report. The ability to route these work files to other analysts or supervisors greatly facilitates the coordination process and thus serves to compress the production cycle. In addition, the intelligence agencies will more effectively respond to ad-hoc requests for information through the more efficient on-line composition and coordination available in SAFE. This is particularly true for the complicated coordination process involved in structuring the input to national intelligence documents.

SAFE will support greater resource utilization through the collection of system management data. This will permit improved system performance and more efficient support during crisis operations.

In summary, SAFE represents a much needed set of processing tools to assist the analyst/manager in producing finished intelligence for national level policy makers.

C. SAFE AUDIT FINDINGS

The SAFE Preliminary Design Review (PDR) convened in January 1982 focused upon those requirements to be satisfied as part of the first SAFE delivery to CIA. This requirement set primarily concerned the message analysis and dissemination software used to support the processing of external electrical message traffic and the dissemination of the electrical traffic to individual mail files. The remaining PDR requirements

involved the capability to: generate personal as well as shared index record and text data files, route textual data to other users, and provide a standard user interface (SAFE User Language) which allows the user to search and maintain these files on-line.

The SAFE PDR provided the CSPO a major opportunity to utilize contractor provided documentation to assess the progress of the SAFE design activity. This documentation identified several major design issues while at the same time provided the government an indication of deficiencies in the initial SAFE software development approach. Because schedule slippage had already occurred and cost overrun appeared imminent, the government decided to perform an audit of the SAFE Project. The audit initially focused attention on those technical and management issues identified during the PDR review cycle. Specifically, the audit team focused on the fidelity of the SAFE design to the stated functional requirements. However, the audit team also addressed the ability of the SAFE development approach, as evidenced by PDR, to satisfy the total range of SAFE requirements including the unique DIA system requirements. These requirements involved the Data Base Management System (DBMS) needed to support DIA's structured intelligence data bases. SAFE affords DIA the opportunity to redesign and restructure its production data bases to reduce data redundancy, insure data base integrity, and facilitate on-line data base maintenance and retrieval.

The SAFE Audit Report was produced by a team consisting of eight personnel from the two parent organizations of the Consolidated SAFE Project Office (CSPO) - the CIA and the DIA. The audit team consisted of ADP managers, computer and communications technicians, and user representatives. The audit report was critical of both the contractor and government in three areas: management, cost/schedule, and technical. The problems identified were:

1. Management

- a. Insufficient management authority was exercised over the project.
- b. The system development methodology was ineffective in quality assurance, installation planning and configuration management matters.
- c. Inadequate resources were applied to the DIA requirements (SAFE-C for CIA and SAFE-D for DIA systems should be developed in parallel).
- d. There was a lack of user involvement, precluding user experience from being fed into the development (requirements) process.

2. Cost/Schedule

- a. The project lacked a realistic project plan.
- b. A lack of commitment to meet delivery schedules existed.
- c. Cost growth was not adequately contained.

3. Technical

- a. The development approach was high risk in terms of cost and schedule, the design and technical problems were believed to be so severe that the development approach could not produce the intended system.
- b. More use should have been made of available commercial software and software currently operating within the government.
- c. Alternative communications subsystem approaches should have been considered.
- d. Hardware intensive solutions should have been preferred to software intensive solutions to reduce risk.

SECRET

III. SAFE OPTIONS CONSIDERED

A. Methodology in Evaluation Process

Upon completion and report of the SAFE audit, CSPO set about to review alternative development approaches which considered delivery schedules, requirements and hardware architectures. These approaches were:

- 1) the continuation of a major software development effort (on Burroughs hardware) but with an attempt to reduce risk, and with provision for an early capability,
- 2) a software integration effort which would emphasize the use of off-the-shelf software in an IBM-compatible environment,
- 3) a mix of the two approaches, where the Burroughs equipment is used to handle terminal connectivity and potentially, the mail dissemination function, and
- 4) a Honeywell hardware architecture (the DIA DIAOLS systems currently operates on this hardware).

The study concluded the only two approaches that could be adequately addressed in the time available would be an off-the-shelf software integration effort using IBM-compatible equipment and continuing with a software development effort in a Burroughs environment. To understand the differences between the two approaches, the distinction between software development and integration should be clearly delineated. Software development within the scope of a project such as SAFE entails full adherence to aerospace engineering methodology for the development of software. Guidance for this is contained in a series of military standards and specifications (MIL-STDs and MIL-SPECs), most notably 483 and 490. This process involves detailed specification generation followed by design, coding, testing, and integration activities and documentation. All work is original and funded by the government. Significant operational readiness tests are required prior to release of the software for use in order to guarantee that all significant software design and implementation problems that would affect system reliability and availability have been solved. A software integration approach makes as much use as is possible of available software products to meet system needs. It is not necessarily the case that this software has been built to aerospace engineering standards but rather that considerable practical experience with the product exists to assure that it performs as advertised and is reliable. The software documentation usually is not in compliance with these engineering standards but the vendor of the software package is capable of providing significant maintenance support

SECRET

(or will allow this support by a third party). Software integration, to the extent that it is done and represents original work, is performed to aerospace engineering standards.

The CSPO staff was divided into two teams to do detailed investigations of the alternatives. The team studying the software integration approach was augmented with personnel from the Office of Data Processing (ODP) in the CIA and an ODP contractor. The software development approach team was augmented with a CSPO consultant.

At the same time, the SAFE contractor, TRW, was tasked with four related studies. TRW was directed to generate the following proposals for an integrated SAFE system:

- 1) a solution using Burroughs hardware and major software development (basically continue as is but reduce the risk);
- 2) a similar solution using IBM-compatible hardware;
- 3) an IBM-compatible solution with an early capability followed by an integrated system yielding the full SAFE, and;
- 4) a solution which utilizes IBM-compatible equipment for CIA and Burroughs equipment for the DIA.

The studies were to address the hardware and software design, the use of available software, the necessary system integration, the management approach, the system costs, and the risks involved with each system.

Certain assumptions were made by both teams, namely the same number of users would be supported by each architecture; the development facility would be moved from the West Coast to the East Coast; the DIA portion of SAFE would be developed in parallel with the CIA portion; and an Early Capability would be provided for some SAFE users to allow them to become familiar with SAFE-like functions and to provide feedback to guide later system development.

Since the software integration approach team was aware of the Pilot Mail Operation (PMO) system in use at the CIA, it was decided that the operation of that system would be reviewed. PMO is being utilized on

IBM-compatible hardware and presents many SAFE-like functions to its users. It was decided to use this software package as a base for software integration. Due to the limited time, packages that team members were familiar with were reviewed for their applicability to the SAFE system in a limited preliminary review. Each package was reviewed by the team to assess whether it fit into a system with other packages and the IBM-compatible hardware.

TRW performed similar tasks and reported their findings to the team chief. This information from TRW was utilized in the research of software packages. Information about TRW-developed software which could be used in the integration was also considered. A decision was reached about which packages to propose for system integration and then schedules, costs, and risks were determined. This information was presented to the system development team and TRW for assessment.

The software development approach team also reviewed existing packages that perform SAFE-like functions. The team worked closely with TRW to accelerate the scheduled delivery of designated SAFE functions. TRW manpower loads and schedules were primary concerns for this development approach. After packages were selected for an early capability, the team determined whether or not to replace these packages with newly developed software for the long-term system.

After the completion of the studies, presentations were made by the teams and critiqued. This process continued until the proposals were accurate and as thorough as time would allow. After completion of the proposals, team members made presentations to the entire CSPO for additional evaluation. The final two proposals were incorporated in one briefing with a recommendation. This package and the recommendation were then presented to senior managers of the parent organizations.

B. RESULTS AND CONCLUSIONS

1. Software Development Approach

(Burroughs Environment)

The solution from the software development approach team updated the design which was provided during the prior three years of work by TRW and added early capabilities through the integration of existing and

available software. Parallel developments for SAFE-C (CIA) and SAFE-D (DIA) were also proposed by the team. The development of the C and D systems is divided into an early capability, an enhanced capability, and integrated capability phases. The development of a fully integrated SAFE system would be based upon an existing commercial mail package and a storage/retrieval system used in the early phases of operation. These packages would be replaced and/or enhanced during the latter stages of operation with software that would be developed by the contractor. Large-size Burroughs processors (B7800) and mid-size processors (B6900) were proposed by TRW for the current development of the SAFE system. TRW's study recommended the use of B7900 machines, an unannounced Burroughs product. Both types of processors use the Monitor Control Processor (MCP) operating system. The team proposed the same hardware and operating system for the development of the SAFE system.

a. Early Capability

The early capability system (April 1983) for SAFE-C would consist of the integration of a commercial mail package called UCSC Mail Dissemination System, developed by University Computing Services Corporation (UCSC) of Delaware, and a document storage and retrieval system called SOLIS, developed by NSA. These packages would be installed on the existing Burroughs machines. Automatic analysis of incoming messages could begin. Mail dissemination and simple indexing functions are provided to the users with a subset of the SAFE User Language (SUL). The users would also be provided with the capability of document file inversion search. The system for SAFE-D would consist of the UCSC Mail Dissemination System only. The System would provide a test bed for some DIA users. The users would also be provided the opportunity to become familiar with Burroughs operational environment.

Both systems would be located at the CIA facility. The hardware for SAFE-C would consist of two B6930s and one B7821. The B7821 and one B6930 would be connected with the Inter-Computer Communication System (ICC), developed by the Burroughs Corporation for SAFE. The other B6930 would be a backup machine that could be connected to the B7821. The SAFE-D system would consist of three B6930s. Two machines would be connected via the ICC and the third machine would serve as the backup unit. These configurations would support 128 concurrent users for SAFE-C and 64 concurrent users for SAFE-D.

~~SECRET~~

b. Enhanced Capability

Additional capabilities would be provided to the SAFE-C users in January 1984. Enhancements would be made to the software packages. The External Message Processor (EMP) would be modified to handle additional message zones. Enhancements would be made to the system to allow inverted search of index files, vocabulary browse, and the ability to search for words in text by using DON'T CARE designators. Text composition capabilities would be introduced to the users and the SUL subset would be extended.

c. Integrated Capabilities

The integrated SAFE system would be provided to SAFE-C users in July 1984. The mail package which was used in the first two phases of system development would be replaced with newly developed software at this time. The system would provide the capability to create a central system catalog and a central document file for indexing. Later, additional capabilities would be added to the system, such as EMP enhancements, document file maintenance, and transaction files. Command procedures, sleep, full controlled access, alerts, and route file capabilities would also be added to the system.

Structured file support with full DBMS capabilities would be introduced to the DIA users in April 1985. With the introduction of the DBMS, conversion of the DIA files could commence. Some additional capabilities which would be provided by the system during this phase include batch capability, canned queries, on-line maintenance, output forms, and geographic search. During the next two years, functional capabilities would be added to the systems until all SAFE requirements are included.

The final hardware configuration for both installations would consist of four B7900's and four B6930's. The upgrade from the B7800's to the B7900's would be needed to handle the increased user population.

2. Software Integration Approach

(IBM - Compatible Environment)

Existing software products which are presently being used in the CIA were postulated for use. The existing Pilot Mail Operation (PMO) was proposed as a base for the SAFE development. The present capabilities of PMO consist of dynamic mail dissemination by user profiles, mail file browse,

~~SECRET~~

SECRET

highlighting of terms, MIS data generation, and routing messages from mail files. The mail file consists of data that are collected over a five-day period.

Additionally, the CIA's Automated Information Management (AIM) electronic mail software package was evaluated. This package was developed by ODP's Systems Programming Division. It was considered for incorporation into SAFE to support the route function and to store index records.

Software packages which meet SAFE requirements would then be procured and installed. Missing functions would be implemented and integrated into the system with the end result being the SAFE system. The existing SAFE User Language (SUL) would be implemented so as to access the multiple processors and functions in the distributed architecture with a single log-on.

The development of the integrated SAFE system was divided into three implementation phases. These phases are the Early Capability, Enhanced Capability, and Integrated Capabilities. For purposes of estimates, IBM 3081 series processors were proposed as the hardware for SAFE development and operation. Multiple Virtual Storage (MVS) and Virtual Machine/Conversational Monitor System (VM/CMS) operating systems were proposed for development and production system software environments. Both operating systems are currently being used at the CIA. MVS provides support for batch usage and for multiprocessing in a large virtual storage environment. VM is a system which provides each user with the functional equivalent of a dedicated computer system (a virtual machine). CMS, the operating system for the virtual computer, is virtual storage-based and provides a general-purpose user interactive capability.

a. Early Capability

The proposed Early Capability system (March 1983), using IBM-compatible hardware, consists of the existing CIA software products PMO and AIM. This would support 300 users (150 concurrently) from the CIA in intelligence production. This system would be duplicated and used by up to 300 DIA analysts.

Hardware for the CIA and DIA users during this phase would be installed at the Site-C facility. The Early Capability phase would supply DIA users with an evaluation system so that feedback could be obtained and considered in later decisions. Functions which would be satisfied during the Early Capability phase include message receipt, mail distribution, mail browse, message routing, and the ability to create and update private index files.

SECRET

SECRET

During the project planning and procurement period for the Early Capability, an evaluation phase and system design phase would be performed for the Integrated Capabilities. Studies of applicable software packages would be performed. Commerical packages for Data Base Management Systems (DBMS) and electronic mail would be reviewed. The packages which best satisfy the SAFE functions would be selected for integration during the latter phase of SAFE development. These studies involve selecting the packages and defining the software augmentations required to meet the functions and to achieve the integration of the packages into the system.

The hardware for the Early Capability phase would consist of the equivalent of an IBM 3081 Model D processor with MVS and another 3081 processor which contains VM/CMS. The AIM package would execute in the VM processor. This package would be used for electronic mail functions. PMO would execute in the MVS environment to provide a private indexing capability and mail functions. The two processors would be connected by using the COMTEN front-end communications processor. This configuration is duplicated to support DIA users. A stand-alone processor containing the MVS operating system running in a virtual machine under VM would exist for development, testing, and integration. A separate processor for backup was also postulated.

b. Enhanced Capability

By October 1984, enhancements and integration of PMO and AIM would be completed and incorporated into the Early Capability systems. This is proposed as the Enhanced Capability phase. The concurrent user population would be increased to 250 for each agency. The processors for SAFE-D would be installed at the new DIA building for DIA usage. Hardware configurations at both sites would be identical. Each site would continue to have the equivalent of two IBM 3081D processors with VM, one serving as backup, and one processor containing the MVS operating system for a private file indexing capability and for message analysis and dissemination.

AIM and PMO would be integrated to run in the VM/CMS environment. Profiles which are used for dynamic mail dissemination could be created and maintained on-line. This would provide the users with the capability to browse their index files. The integration would result in one log-on to access the packages instead of the two previously necessary. The mail dissemination analysis process that was designed and tested in the Burroughs environment would be integrated into the system to run on the MVS processor.

c. Integrated Capabilities

Using a commercial Data Base Management System (DBMS) with augmentations, the CIA and DIA files would be converted and placed into operation. By the end of 1985, each site would have three large machines networked together with a fourth machine used as a backup. Additional modifications and enhancements would be made through 1986 to fully meet the SAFE requirements.

Up to five hundred concurrent users (one thousand total users) would be supported during the integrated capabilities phase of operation at each site. An additional processor would be procured for each site, and all processors would be upgraded to Model K. The hardware configurations would then consist of the equivalent of two 3081 Model K's with VM/CMS, one 3081 Model K with MVS, and one 3081 Model K with MVS running under VM. The VM/MVS processor would serve as a backup machine also.

Enhanced mail pre-processing and analysis functions would be added to the MVS processor. This mail analysis process would provide some enhanced zoning capabilities. Data Base Management Systems would be installed to support structured and document files. Most of the DBMS's which are being reviewed in the evaluation activity run under MVS. Only one log-on would be required to access all SAFE functions during this phase of operation. Combined text search and inversion capabilities for retrospective searching would also be provided during this phase. The development of SAFE would then be complete and the project would become mostly operations and maintenance.

3. Risk Assessments of Approaches

a. Software Development Approach

It was concluded that the integration of the available software packages for the Early Capability presented a high risk due to inexperience with the software. Further, the development of a data base management system using Burroughs systems software to meet the DIA requirements presented a high risk. This development used DMS-II (the Burroughs DBMS) primarily as the data access method. The complexity of the network structure required to integrate the Burroughs hardware into a fully operational system presented a high risk. The development approach was judged to be at high risk since it was characterized by considerable software development.

b. Software Integration Approach

The risk assessment for this approach was determined to be low for the Early Capability because the software is currently in operation at the CIA using IBM hardware. The risk for DBMS development is low because it would be based on a commercial product better matched to SAFE's needs with fewer required

augmentations. However, the integration of the DBMS into the SAFE system would present a high risk due to the unknown enhancements and modifications that might be involved in this process. System performance might suffer when the software is integrated. However, the availability of large capacity, high speed machines alleviates this problem. Networking of only four IBM-equivalent machines presents a lower risk than networking eight Burroughs computers. There are existing machines in the ODP computer center where some networking has already been performed. The reduced amount of software which may have to be developed for the software integration effort presents a lower risk than the much greater amount of software which must be developed for the software development solution. Therefore, the integration solution was considered to present a lower risk than the software development approach.

C. COMMUNICATIONS OPTIONS

In support of both basic options, an analysis of alternative terminal communication subsystem approaches were performed.

The SAFE terminal communications requirements specified a need to pass textual data between the end user and the computer complex. While there is a need for sophisticated graphics support, the bulk of the requirement is beyond the scope of the current SAFE program activity. The requirements, in their simplest form, can be expressed as a need for 9600 baud, full-duplex communication supporting the full user population.

A cost analysis associated with completing the current Wide Band Communications System (WBCS) was performed. Two forms of this system are required: a Black System (containing an integrated cryptographic overlay) for the CIA and a Red System (without the overlay) for the DIA. It was estimated that the cost to the SAFE program to complete the WBCS including acquisition and installation for both agencies was between \$20 to \$25 million.

No commercial broad band bus communications system could satisfy the SAFE requirements without further development. Integrating the cryptographic overlay would add additional cost and risk for this approach. A baseband system would require extensive modification to the cable system installed at CIA.

Since both agencies were pursuing the installation of twisted wire pair, point-to-point communications (the CIA proposed a large expansion to their current grid and the DIA proposed installation of wire pair in the DIAC), this option was

considered. It was determined that this latter approach would be responsive to SAFE requirements and would cost the SAFE program on the order of \$1 million.

Therefore, both options elected twisted wire pair, point-to-point communications as part of their solutions to the SAFE requirements.

SECRET

IV. MANAGEMENT APPROACH FOR REDIRECTION OF SAFE

A. INTRODUCTION AND EVALUATION

Both teams recognized the need for a major change in the approach to delivering the SAFE system and for major management changes within TRW's SAFE Project Office and within the government's project office if the SAFE project is to succeed.

Effective tools for risk management must be employed. Initial action in this area is to opt for buying software packages already available in the marketplace and tailoring these where required to meet SAFE requirements. User experience with the early capabilities provided by existing CIA software will allow feedback to avoid costly development of unnecessary software. Where off-the-shelf packages do not meet SAFE requirements, trade-offs can be made to determine whether to build software from scratch, modify existing packages or wait for the marketplace to develop the package (capability) in question.

Table I shows further risk reduction by using a hardware intensive (integrated software) architectural solution instead of a major software development solution. The chart shows that in the software integration approach, approximately 70% of project funds are invested in hardware while 30% is in software (primarily in integration and package enhancement). For the software development approach, the software situation is reversed, 70% of the cost is in major software development and 30% in hardware procurement.

Table II further illustrates this by showing a comparison of the contractor manpower needs, showing a peak of 360 for the software development approach while showing a peak of 170 for the software integration approach.

Both the government and TRW have replaced their project managers. The major activity relating to the integration of the software packages and enhancing these packages, where necessary, will occur on the East Coast instead of the West Coast. This will allow much greater government participation in the resolution of design issues and prompt assertive management and contract monitoring by the government. Government teams and contractor teams will be aligned to designate responsible individuals for successful completion of specified tasks.

Project Planning will be supported by clearly defined milestones and detailed schedules. Cost accounting on resource expenditures will be reported monthly.

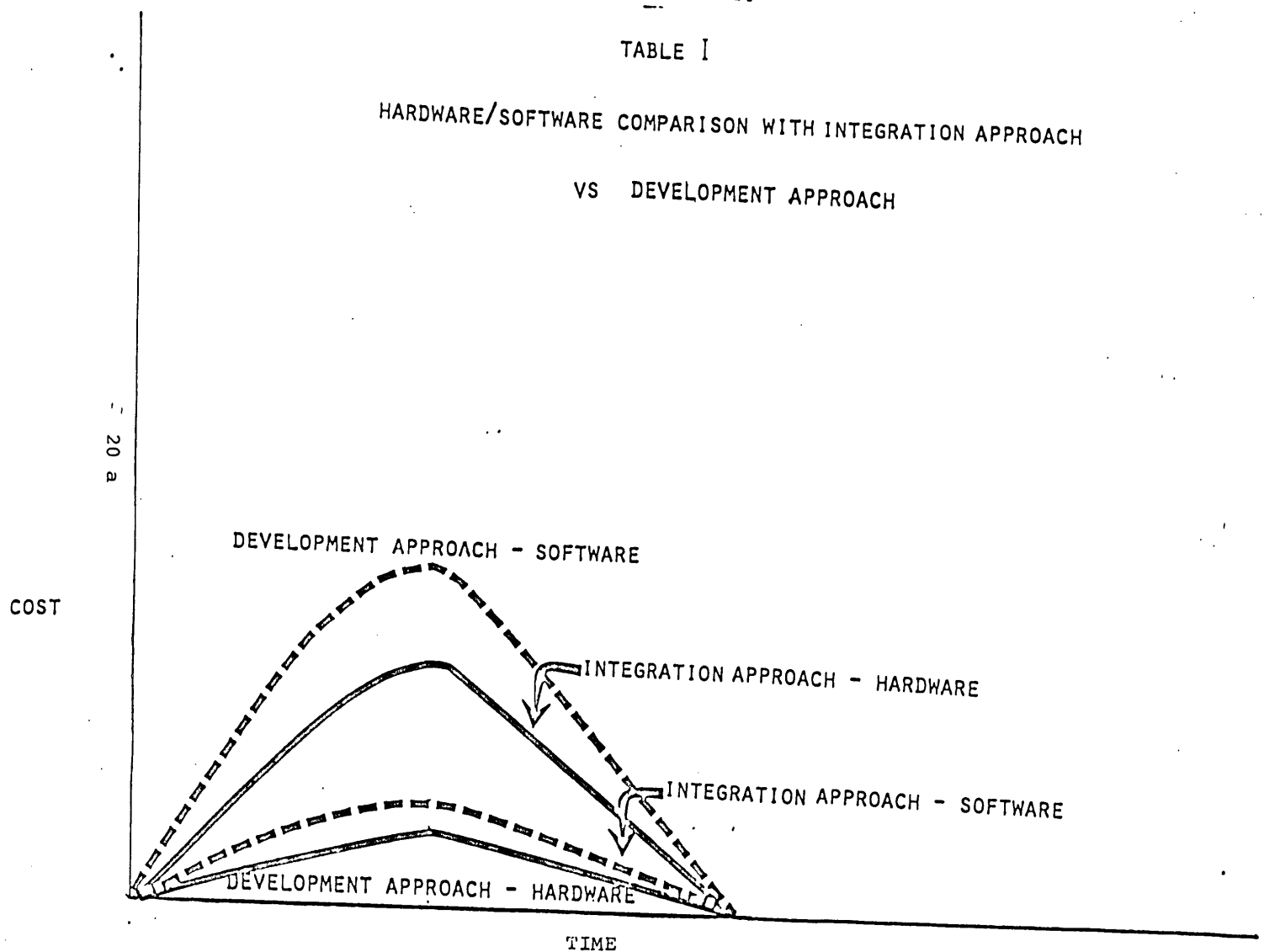
SAFE will no longer be managed by a committee. Senior individuals within both agencies will be (identified as) responsible for the successful completion of SAFE. These officials will receive frequent status reports and briefings on SAFE progress and problems. These briefings will include as a

SECRET

~~SECRET~~

TABLE I

HARDWARE/SOFTWARE COMPARISON WITH INTEGRATION APPROACH
VS DEVELOPMENT APPROACH



~~SECRET~~

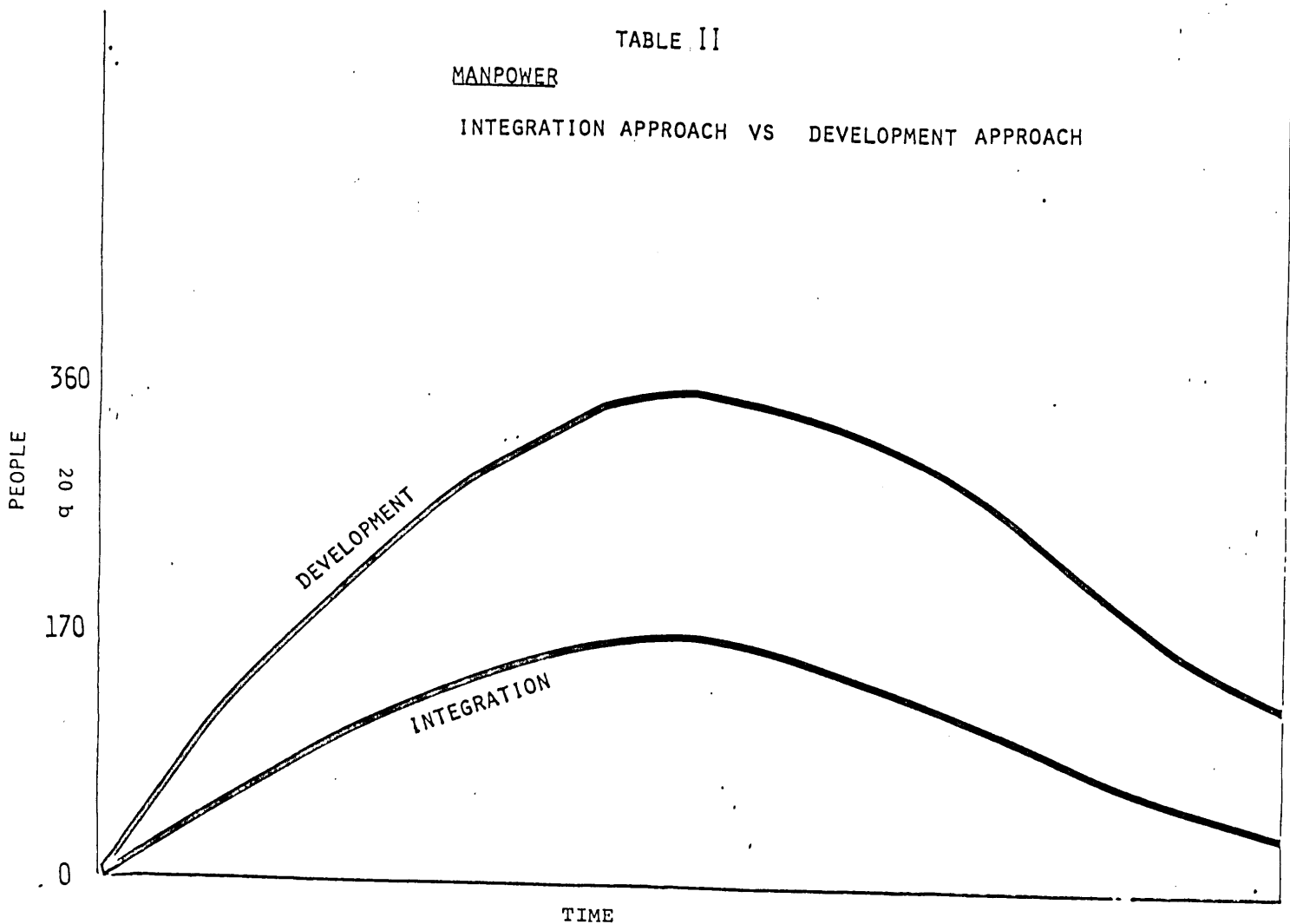
SECRET

Approved For Release 2006/08/17 : CIA-RDP83M00914R002000190004-0

TABLE II

MANPOWER

INTEGRATION APPROACH VS DEVELOPMENT APPROACH



SECRET

Approved For Release 2006/08/17 : CIA-RDP83M00914R002000190004-0

SECRET

minimum progress against planned milestones (PERT), financial expenditures against planned resources, problem areas (design issues) and problem resolution.

A strong validation and verification (V&V) contractor will be employed by the CSPO to assist in maintaining a baseline configuration, to insure that quality assurance standards and procedures are properly followed, and to assure requirements are being satisfied.

Hardware will be procured directly by the CSPO thus avoiding third party overhead and fee.

A systems integration contractor will be employed to directly assist the CSPO Project Director and Deputy Director in resolving technical issues and in providing assertive management to insure all the pieces of SAFE are coming together into a viable system responsive to the needs of the intelligence analysts of both agencies.

B. LINE MANAGEMENT OVERSIGHT AND COORDINATION

In response to the criticisms of SAFE program management made by the audit team, a number of changes have been made and others are proposed. As a result of the CSPO evaluation presented in the first part of this section, the following paragraphs outline the management approach proposed by CSPO and their line managers.

The responsibility for the development of SAFE within CIA will belong to the Deputy Director for Administration (DDA) and within the DIA to the Assistant Director for Resources and Systems (RS). The Consolidated SAFE Project Office remains the executive agent for the development of SAFE. Reporting to the DDA will be through the Director of Data Processing for CIA and to the DIA/RS through the Deputy Assistant Director for Defense Intelligence Systems (RSD) within DIA. Coordination with the user communities and appropriate data processing organizations within both agencies will be the responsibility of the CSPO. The Steering Committee established by the original agreement between the two agencies will be abolished. Quarterly reporting to the Deputy Directors of the two agencies will be provided.

C. CONSOLIDATED SAFE PROJECT OFFICE (CSPO)

The Consolidated SAFE Project Office remains jointly staffed by the CIA and the DIA with program management as specified in the Memorandum of Understanding and the attendant SAFE Management Plan which established CSPO. The CSPO will be organized into three segments: Quality Assurance, System Development and Operations Support. (See Table III) This is responsive to the fact that SAFE is to be developed incrementally. Quality assurance and configuration management shall be emphasized to guarantee smooth transition between increments with minimal disruption of service to the users.

TABLE III
Approved For Release 2006/08/17 : CIA-RDP83M00914R002000190004-0
CONSOLIDATED SAFE PROJECT

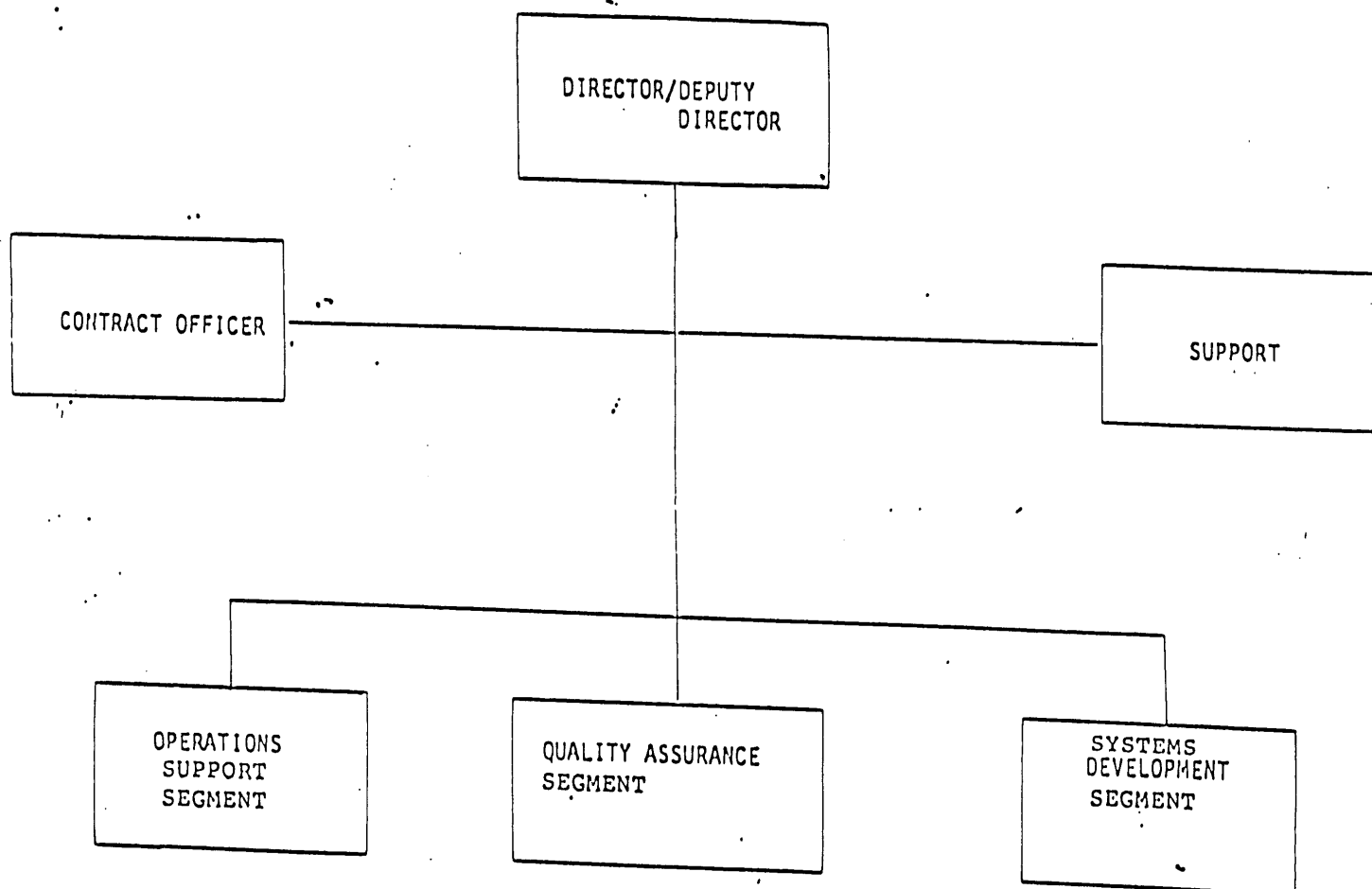


TABLE III

1. Quality Assurance

The Quality Assurance (QA) Segment will maintain all software and documentation baselines. The QA segment will also maintain liaison with user organizations within both the CIA and the DIA. There will be a single point of contact within the DDI/CIA and VP/DIA for user requirements. Areas of liaison will include training requirements, terminal allocations, user feedback, and user language scenarios.

The QA organization will provide executive secretary support to the project's Configuration Control Board, which will be chaired by the Director of the Consolidated SAFE Project Office. The Board will consist of senior engineering and user representatives of both agencies. On engineering matters, the Deputy Director of CSPO will represent the DIA and the Chief of the System Development Segment will represent the CIA. On requirements matters user representatives from the two organizations will speak for the user communities. This segment will use contractual support for the various quality assurance functions, to include design validation and verification.

2. System Development

The System Development Segment will manage a contractor who will be responsible for the delivery of increments of capability to the users. This process involves the identification of software packages that provide some portion of the SAFE functions. A software package may require augmentation to achieve the desired functional capability. In turn, a set of packages may require integration to achieve some composite set of functions, called an application, service, or capability (e.g. mail handling in all aspects - analysis, dissemination, indexing, and viewing). The services will then be integrated into a delivery. The development of each delivery will be monitored by the QA Segment for adherence to the project standards and responsiveness to requirements; it will be baselined upon acceptance and then turned over to the Operational Support Segment.

The individual software packages, applications, or services will be provided to and managed by a development contractor who will assure their integration into a system. The contractor will address all aspects of a delivery including user interface integration, testing, file conversion, software installation, user support documentation, etc.

Since the focus of the development approach is on what the marketplace can provide and on software integration, rather than software development, the software package selection, augmentation, and integration activities are all elective tasks and are not mandatory. The implication of this is that the proper structure of the contract with the software integrator is

a task-oriented one.

3. Operational Support

The Operational Support Segment will be responsible for the operation and maintenance of a delivery. Upon acceptance by the QA Segment and the Operational Support Segment, users will be introduced into the new system environment. Operations and maintenance contracts will be written and executed by this segment. This segment will also be responsible for providing assistance to the users in the event of system problems. Most problems will be corrected by this segment and reported to the QA Segment. Problems too severe to be corrected by this segment will be identified to the System Development Segment so that corrections to these problems can be incorporated into subsequent deliveries.

As the proposed development approach for SAFE does not entail hardware development and only hardware procurement, the government will provide the necessary equipment directly. In fact, the acquisition of equipment for the SAFE computer centers is nearly identical to the acquisition activities of the Processing component of the Office of Data Processing. To the extent that the systems software (i.e. VM and MVS operating systems) required for SAFE represents an acquisition, rather than a development activity, this organization is highly experienced in providing this software.

D. INTEGRATION

It should be noted at this point that a clear delineation of the two integration roles is fundamental to understanding the responsibilities outlined above. First, there are certain activities that can be generally defined as software integration. These activities encompass the melding and testing on several levels of various pieces of software that make up a system. These levels range from the interweaving of small pieces of software into modules followed by the aggregation of modules into applications and finally the orchestration of the applications into a system.

The second type of integration can be referred to as systems integration, which assures that new systems are introduced into an operational environment with maximum coordination and minimal disruption.

In the management approach suggested here, the development contractor will be solely responsible (with V&V oversight) for software integration. The CSPD will employ a separate contractor to fulfill the systems integrator function.

E. SOFTWARE MANAGEMENT

The SAFE software management will be conducted according to consistent and effective software management practices. These practices used for management assessment and control are described in the development phase activities set forth in this section and represented in Table IV. The major SAFE software development phases consist of:

1. User Design Review (UDR)

A User Design Review will be held to review the User Manual and the User Interface Specifications. These documents are major inputs to the System Requirements Specification and to the Acceptance Test of the system.

2. System Design Review (SDR)

The System Design Review will be held to review the System Design Document, System Test Plan, Hardware Configuration Specification and Computer Program Configuration Item (CPCI) Criteria/Interface Specification. A CPCI may be routines, programs, groups of programs or an entire software subsystem (if sufficiently small). The aggregate of CPCIs is the software system. These documents and specifications are major inputs to the preliminary design and integration test phases.

3. Preliminary Design Review (PDR)

The Preliminary Design Review will be held to assess the design, schedule, cost and risk of each vendor augmentation and TRW CPCI Augmentation Specification. The Preliminary Design Review provides input to the Critical Design Review.

4. Critical Design Review (CDR)

The Critical Design Review will be held to review the "build-to" designs and test plan for each CPCI and the Integrated Test Plan for all CPCIs. The Critical Design Review provides input to the development test phase.

5. Development Test

The Development Test phase comprises the coding, testing and CPCI integration. It results in the "as-built" description of each integrated CPCI and in the input to the Integration Test Phase.

6. Integration Test

Integration Test consists of the integrated capabilities testing of system capabilities as defined in the System Design Document produced at System Design Review (SDR) and

DEVELOPMENT APPROACH TO INTEGRATED CAPABILITIES

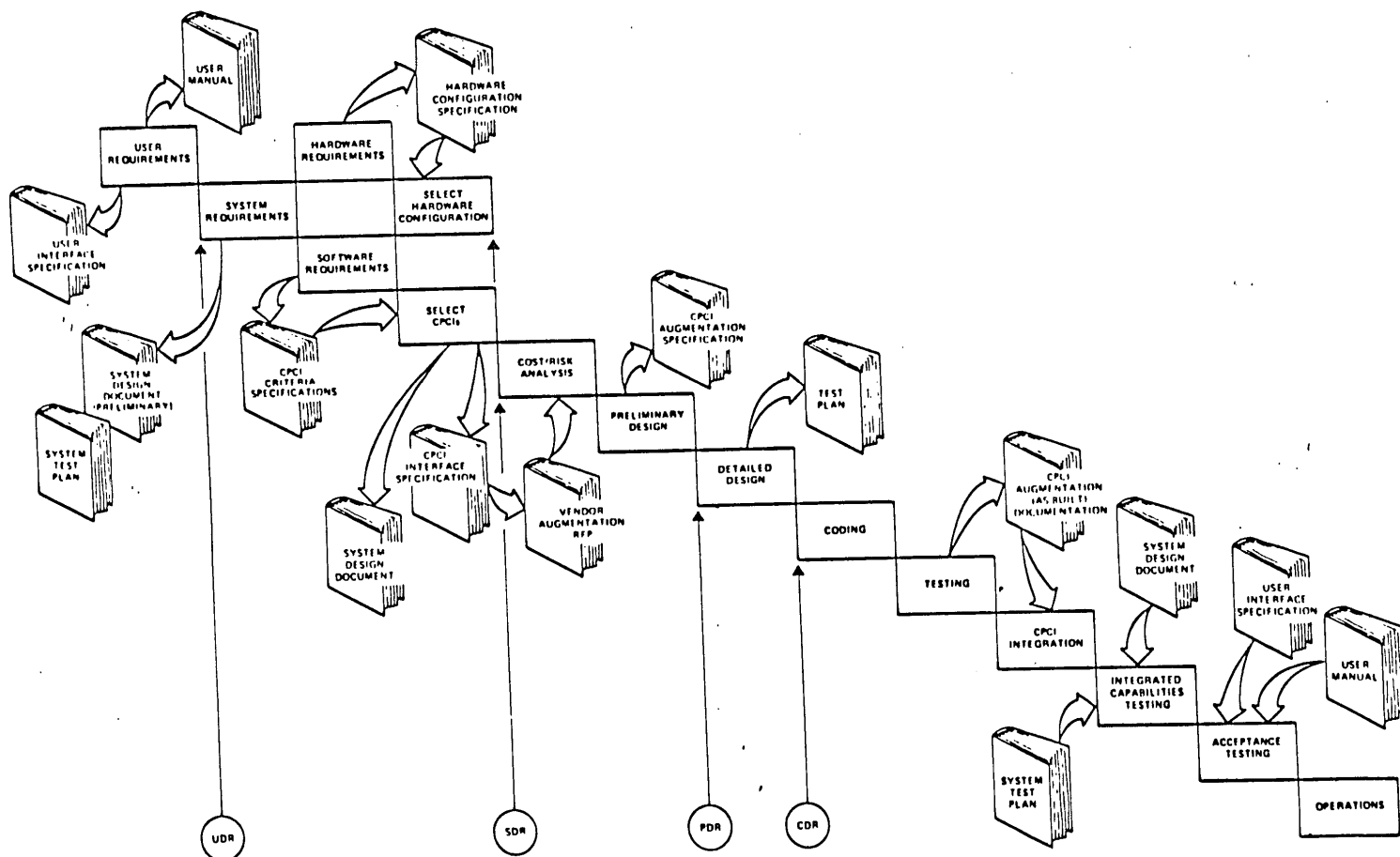


TABLE IV

SECRET

maintained to this phase. Completion of Integration Test is input to acceptance testing.

7. Acceptance Test

Acceptance Test consists of assuring the system performs to the User Manual and User Interface Specification produced at the User Design Review (UDR) and maintained to this phase. Completion of this phase is prerequisite to turning the system over for operations.

F. THE DEVELOPMENT CONTRACTOR

It is considered prudent to continue with TRW as a primary contractor but in a significantly reduced role. Project continuity and understanding of the SAFE requirements are major underlying reasons for continuing with TRW. Despite the shortcomings highlighted by the Audit, over the past three years TRW has developed a unique understanding of what capabilities SAFE must provide. They have exhibited that unique knowledge in the various requirements specifications (e.g., SAFE user language, System requirements, Conversion). In addition, TRW personnel who will be retained on the SAFE project have security clearances that normally require 9-12 months to obtain. It is believed that if a new contractor were introduced to perform TRW's role then a slip of 9 to 12 months would be inevitable before the actual development of integrated SAFE could begin.

TRW's role in the SAFE implementation has already been significantly reduced. The size of their contract will drop from a potential [redacted] This 25X1
reduction is possible through the termination of the expensive 25X1
wideband communications development (projected to cost [redacted] million), by trading major software development for the 25X1
integration of off-the-shelf packages [redacted] 25X1
[redacted] through the closing of the West Coast Development 25X1
Facility and moving to a government furnished facility (CIA) on the East Coast [redacted] and through 25X1
government procurement of hardware instead of TRW procurement (a reduction of TRW responsibility by [redacted]). Other 25X1
reductions to the TRW role involve government contracting directly for an independent verification and validation contractor (a reduction of TRW's role by [redacted]) and 25X1
shifting the overall systems integration (i.e., overall technical direction) responsibility from TRW to an experienced integration contractor who will directly support the Director of CSPO in [redacted] 25X1
resolving management and technical problems (a reduction [redacted]) 25X1
[redacted]

SECRET

V. SOFTWARE PACKAGE SELECTION AND EVALUATION (TASKS AND STATUS)

A. INTRODUCTION

The approach to the development of SAFE adopted by the CSPO recognizes the strong relationship that SAFE has to commercial data processing developments in the areas of office automation, electronic mail, and data base management systems. The approach seeks to determine how the marketplace may best support the SAFE requirements while achieving an integrated environment that is easy for the intelligence analyst to use.

Fundamental to the development of SAFE is (1) maximum use of available software and (2) incremental delivery of capabilities to the users. In order to make optimum use of applicable commercial and government software, an IBM-compatible hardware environment is to be provided. Communications support to the terminals will be by non-encrypted twisted wire pair in order to minimize cost and risk. Twisted wire point-to-point communications already exists at the CIA and is being installed in the new DIA building. Tasks performed during the evaluation phase will result in the selection of software packages to be used as part of SAFE. Each of the software selection tasks includes the determination of what augmentations (and their costs) are required to these packages in order to provide the requested capabilities. Additionally, the studies determine how to put the software packages together to provide the combined set of services. Further, all of the software must function with the computer and communications hardware. The design for these integrated capabilities will be presented at a System Design Review in February 1983.

The costs and schedules to develop these augmentations and the risk of being able to achieve them will be assessed. High risk or high cost augmentations will be weighed against their value to determine if they should be developed. This process also applies to the issue of achieving the integrated user-interface. Where it is deemed that the risks or costs are excessive relative to the value received, augmentations to achieve the user-interface integration will not be attempted. The assessment of the value of augmentation will be made at appropriate intervals, primarily at design reviews throughout the project.

It is expected that the marketplace will be active in solving many SAFE-like problems through improved performance hardware or through software with greater capability. An incremental approach to the development of SAFE allows continuous monitoring of the marketplace.

Once the software package selections, augmentations, costs and schedules have been determined, a project plan for SAFE can be established. This will be available in November 1982.

SECRET

The CSPO is currently developing the detailed plan for providing an early capability. The plan will be available by late September 1982 and is on schedule. This plan will provide for opening the SAFE computer center at CIA in March of 1983. It will contain three facilities: an expanded Pilot Mail Operation for CIA, a separate capability for the DIA (using DIA message traffic), and an unclassified development facility (for integrated capability development).

Since the Steering Committee meeting of 22 June 1982, the CSPO has concentrated on specific tasks critical to the evaluation of the proposed development approach. The evaluation process will continue through September. The objectives of each of the evaluation areas and the status of reviews are summarized below.

B. DBMS Study

The objective of the DBMS selection subtask is to select an IBM compatible Data Base Management System (DBMS) and text handling package that best meets the needs of the SAFE project. The selection is based on adherence to SAFE requirements as defined in the selection criteria. The DBMS is to be selected from the broad spectrum of commercially available products on the basis of their inherent capabilities and their compliance with SAFE functional, maintenance, resource usage and environmental requirements.

If existing software does not cover the requirements, the study will identify enhancements to existing software and/or the need for additional software required to satisfy the SAFE Data Base Management System requirements.

The technical approach for evaluating and selecting DBMS and text packages insures that the systems currently available are considered and makes certain that no promising candidates are omitted. Furthermore, the approach insures that the systems of interest are subjected to a sufficiently exhaustive technical analysis to validate the recommendations and conclusions.

The technical approach to DBMS performance assessment includes effort to design a prototype data base that will exercise the important file structures and relationships for both the CIA and DIA customer. There will be two data bases defined, one for textual data and one for structured data.

An extensive literature search has been conducted which included the DATAPRO and AUERBACH reports, a DATAMATION listing and various internal TRW compilations. The list was screened to select those DBMS packages that are compatible with an IBM environment. This resulted in the identification of 19 structured DBMS's. Separately identified were a list of 14 possible text DBMS's.

..

SECRET

The candidate DBMS's are as follows:

Structured DBMS

ADABAS
BASIS
DATACOM/B
DL/1
GIM-II
GIM-III
GIS/2
IDMS
IMS/VS
INQUIRE
MODEL 204

OASIS
ORACLE
RAMIS-II
SEED
SIBAS
SYSTEM 2000
TOTAL
SQL/DS

TEXT DBMS

BASIS
CONTEXT C-705
COSMIC
DIALOG
DOCU/MASTER
IMDOC
INQUIRE
LEXIS/NEXIS
ORBIT III
STAIRS/VS
SUPER FAST STORAGE
AND RETRIEVAL SYSTEM
TEXT 204
JURIS
ASPEN SEARCH

These DBMS's were analyzed to identify the structured and text DBMS's that will undergo detailed technical evaluation. This was accomplished by applying a set of mandatory requirements to the previously identified IBM compatible packages and then performing a preliminary technical evaluation where necessary to reduce the list to the following:

Structured DBMS

ADABAS
IDMS
INQUIRE
MODEL 204
SYSTEM 2000

Text DBMS

BASIS
DOCUMASTER
INQUIRE
STAIRS/VS
TEXT 204

The familiarization with the DBMS's selected for detailed evaluation has been completed.

Technical meetings were held with the vendors of each of the above packages to gain a complete and detailed understanding of the internal data structures and data access methods employed and to resolve other technical issues that were open as a result of reviewing the technical documentation. Initial performance projections were made based on the information gained.

A second pass evaluation has been performed against the data base management systems (DBMS) on the reduced list against a lengthy and complex set of criteria.

The criteria are categorized as:

Functional - evaluates the end use required of the DBMS.

Maintenance and Vendor Support - evaluates the maintenance and modifications required of the DBMS.

Inherent - evaluates the system integrity and reliability required of the DBMS.

Environment - evaluates the computer interfaces, both hardware and software required by the DBMS,

Resource Usage - evaluates the computer resources used by the DBMS; determines performance aspects of the DBMS,

The results of the second pass evaluation ranks the DBMS's as follows:

Structured Files

ADABAS
INQUIRE
MODEL 204

Text Files

INQUIRE
MODEL 204 (TEXT 204)
BASIS

Additional analysis, as typified by the sample augmentation analysis for Model 204 provided below, will be required to complete this phase of the DBMS selection. A report will be provided presenting the DBMS selection(s) upon completion of the augmentation analysis.

This work will be followed by a design phase during which representative SAFE file structures will be prototyped to determine the proper approach to hosting the file system under the DBMS(s) chosen. Actual performance data will be gathered to determine if there is a need to reconsider the DBMS candidate selections. The design phase will complete with a presentation of the intended DBMS/file system approach at a System Design Review.

Cost data has not been captured yet for most systems but representative data is shown for Model 204:

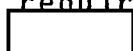
Acquisition Cost:

Basic Package
 User Language
 Host Language Interface
 Utilities
 One T.P. Interface
 Data Dictionary
 Math Pack
 Total license fee
 for the first copy



25X1

There is a 20% GSA discount on the license fee only for government installations. Additional discounts may be available for multiple copies. A minimum of two copies per Agency will be required for an estimated acquisition cost of approximately



25X1

At this point in the evaluation process, it is premature to give definitive answers concerning cost and the degree to which SAFE requirements can be met. Given the fact that the DBMS decision will be one the analysts will have to live with for the next fifteen to twenty years, the goal is to select the best available package based on an overall evaluation which includes what needs to be done to overcome the particular shortfalls of the package. The available list of candidates has been narrowed, however, and it is possible to describe a representative case which will be covered in much more detail as the study progresses. Model 204 is one of the DBMS finalists and significant research has already been done on this product. Although Model 204 may not be the chosen package, it is representative of the class of available DBMS's that would come closest to meeting SAFE requirements. As previously stated, no single DBMS will fully meet our needs. The following is a discussion of these areas where Model 204 is deficient and a possible approach to overcoming the deficiency. If a DBMS other than Model 204 is chosen, the actual deficiencies may be different but nevertheless similar in that a certain important subset of the requirements will not be met.

Capabilities not supported by Model 204 and preliminary estimates of associated cost and risk are shown in Table V, which is an example of the kind of output that will be included in the final report on all software package evaluations. If we decide to implement the changes needed to meet all of the identified DBMS requirements, the cost is estimated to be from [] It should be noted the original development cost of Model 204 is many times these cost figures. It is an advantage of the software integration development approach that only a small fraction of the original development cost is paid by the SAFE program as part of the package acquisition costs.

25X1

Page Denied

Next 2 Page(s) In Document Denied

C. Other Software Package Study

The objective of this task is to identify which packages will be used in addition to the packages selected by the DBMS Study task to provide an integrated SAFE system. We will evaluate both government and commercial packages to determine which can best satisfy the functional requirements of SAFE. If the existing software packages do not cover the requirements the study will identify enhancements and/or the need for additional software required to satisfy the SAFE requirements. These three functional package studies cover the requirements for Mail Dissemination, Non-Mail Applications, and Operating Support Software. In a parallel Software Architecture study we will coordinate the activities of the DBMS study and the three functional package studies and describe how the selected packages will be combined into an integrated SAFE system. The Software Architecture effort will document the design in the software portion of the System Design Document. The document will include a traceability of all SAFE requirements to either existing software packages, augmentations to those existing packages, operating system software or custom software. In addition, the document will provide a description of package interfaces and sequencing, and a technical discussion of both local and system wide issues.

The Mail Dissemination study focuses on packages that can provide SAFE mail dissemination. This basic mail capability will include the following functions:

-Message analysis

The ability to receive electrical messages and interpret and decompose them into zones according to predefined rules.

-Mail dissemination

The ability to match incoming messages against user interest profiles and deliver mail based on those profiles.

-Mail viewing

The ability to format mail for display or hardcopy and to dispose of mail in a variety of ways.

-Indexing

The ability to associate user-defined keywords with a given message and use those keywords for subsequent retrieval of the desired message.

The Non-Mail Application study will focus on packages that provide functional support for a SAFE user. This study will include evaluation of the following functions:

- Text editing
- Word processing
- Special file maintenance
- User interface presentation
- HELP/CAI (Computer Aided Instruction)
- Terminal interface
- Command language parsing/translation.

The Operating Support Software Study will focus on packages that provide functional support for the SAFE operators and for the package integration. This study will identify which package, including the host Operating System, will be used to provide the following capabilities:

- Initialization/Termination
- Operator interface
- Intra- and inter-machine communications
- Failover
- Error collection and reporting
- Health monitoring
- Security processing
- Tape management
- Management Information System (MIS)
- Print job control
- Hardware configuration
- Terminal interface
- ODP link

The Software Architecture study will complete the system design. It will investigate the candidate operating system to resolve potentially critical design issues and to validate the allocation of functions to the operating system. The complete system design will be compiled from the DBMS, mail, non-mail applications and operating support software inputs. Potential functional overlaps, interface discrepancies, and requirements will be identified and resolved. In conjunction with the system engineering studies on design validation (below), we will trace the requirement specifications to specific software packages. The integrated system approaches to critical issues such as data integrity, recovery, security and user language processing will be documented in the System Design Document along with operating system issues such as network communication, file sharing and terminal interface.

1. Mail Dissemination Study

Fourteen mail packages have been identified, twelve vendor provided and two government provided. A list of all 14 is contained in Table VI. A first pass evaluation has been conducted on all fourteen packages, and seven selected (five vendor and two government) for further analysis. They are:

- | | |
|------------------|--------|
| - COMET204 | - TOSS |
| - MAILBOX (STSC) | - AIM |
| - OMNICON | - PMO |
| - PROFS | |

The following areas of functional requirements were met by the seven selected packages:

- | | |
|----------------------|------|
| - Message Analysis | |
| None | |
| - Mail Dissemination | |
| PMO | |
| - Mail Viewing | |
| COMET204 | TOSS |
| MAILBOX | AIM |
| OMNICON | PMO |
| PROFS | |
| - Indexing | |
| MAILBOX | TOSS |
| OMNICON | AIM |
| PROFS | PMO |

A second pass evaluation has been performed against the reduced set of mail package candidates. The evaluation criteria used for this analysis was categorized similar to the DBMS study. The resulting list is:

AIM
PROFS
COMET 204

Since COMET 204 was significantly lower ranked than the first two packages it has been dropped from further consideration.

A systems engineering analysis of the two packages has determined that they should only be considered for supporting the SAFE Route function, the SAFE Compose function, and possibly, mail viewing. Mail indexing shall be included under the DBMS design analysis. Message analysis and message dissemination shall continue to be treated under the design being generated by Operating Systems Division of Logicon Inc. As further guarantee of producing a high performance message dissemination procedure, a design concept proposed by Chase, Rosen, and Wallace, Inc. shall be tested. This algorithm shall be included in the Enhanced Capability Phase of SAFE which is described subsequently in this paper.

Page Denied

The following preliminary cost data shows the range of prices for this kind of software:

- COMET 204(CCA) - \$57K/computer if purchased alone
\$35K/computer if purchased with DBMS M-204
- MAILBOX (SISC) - \$40K/computer
- PROFS (IBM) - No purchase cost; rental \$370/mo
for each computer
- TOSS (NBS) - \$7,200/computer

2. Non-Mail Application Study

The survey of available packages has produced an initial set of eleven which cover the following areas of functional and derived requirements:

a. Text editing/formatting

ATMS: An IBM product which supports text entry, editing, formatting, storage and retrieval of documents. This package supports an interface to STAIRS (text search package) and the IBM DCF formatter.

DCF: (Document Composition Facility): and IBM product which provides text formatting.

DLF (Document Library Facility): an IBM product which provides document storage and retrieval by name.

WYLBUR: A Rand Corporation product which provides text editing with extensive macro features.

b. Command language/user interface/maintenance

QBE: (Query by Example): an IBM product which provides an interface to support searching, sorting, creation of files, maintenance and browse.

IXF: (Interactive Extension Facility): an IBM product which provides a general purpose menu-driven interface to application software.

c. HELP/CAI

Interactive Instructional Authoring System: an IBM product for generating CAI-type instructional material.

Interactive Instructional Presentation System: accompanies the above to provide a system for presenting instructional material.

d. General Packages

SyncSort: produced by SyncSort Inc. as a general sort/merge package.

DMS (Development Management System): an IBM product which provides support for developing applications to run under CICS.

IMS/ADF:(Application Development Facility): an IBM product which provides support for developing data base applications.

Assessment of these packages indicates:

None of the text editing packages provides any significant benefit over that provided by SCRIPTX and XEDIT; both available under the VM operating system;

User interface support packages will be considered with the user language/user interface task, described following;

The CAI packages are available presently within the ODP system although they are not being used at present;

Software development packages do not support all user needs and this consideration is premature. Therefore it has been decided to suspend further work on the Non-Mail Applications Study at this time.

D. User Language

A User Language Specification (ULS) was produced and delivered on 10 May 1982. It contained the majority of the user interface and commands for the CIA user. The emphasis of these activities is to complete this work for the DIA user. The set of user interface issues to be addressed for DIA and the approaches to be taken for each, are being generated and coordinated with CSPO before detailed updates to the ULS are performed. These additions are to be derived from the DIA unique functions identified in the system requirements specification.

In addition to the ULS baselining, a set of user interface scenarios will be prepared to demonstrate and validate the language. These scenario definitions will be a joint effort of TRW and CSPO, and expand the set already prepared by TRW.

Preparations for the baselining of the ULS are well underway. A list of the DIA capabilities that need to be addressed for the ULS has been generated and implementation approaches are being considered. Two of these approaches, for linked file search and geographic search, have been prepared and will be coordinated with CSPO. An analysis has been performed to determine what issues must be resolved before the user interface can be implemented. These are subject to coordination and prioritization before updates to the ULS are generated. A preliminary analysis of the software studies has been performed to determine a list of areas which are highly subject to change based on the pending selection of vendor software packages.

Software packages being evaluated in the DBMS, Mail, and Non-Mail Studies will be analyzed to determine their ability to provide the SAFE user interface. If existing packages do not cover the requirements, enhancements or translations will be identified. This task will support the evaluation of appropriate software packages, support the identification of enhancements, and support identification of cost schedule and risk assessment associated with each enhancement.

E. Requirements Closure

The objective of the Requirements Closure Task is to update and baseline the system level requirements. The technical approach includes coordinating all currently identified requirements issues pertaining to these specifications with the CSPO and update the specifications to reflect the corresponding changes. Incomplete requirements in the areas of the DIA communications systems interfaces will also be specified. The requirements will then be allocated for implementation in a specific delivery. As continued software package evaluation and trade-off analyses are performed and requirements changes are directed by the CSPO, the specifications will be updated to reflect these changes.

The most significant aspect of the open requirements is the area of the DIA communications systems interfaces. The message systems interfaces are being addressed with the development of the Early Capability, described elsewhere in this paper. The interface of DIA SAFE to the DODIIS network shall be determined during the design phase but prior to the System Design Review.

All open (i.e., prior to the redirection) System Requirements Specification changes has been reviewed. TRW has been directed to prepare the appropriate Specification Change Notices to update this document.

F. Conversion Analysis Support

The objective of Conversion Analysis Support is to specify the requirements for data base and program/product conversion (conversion of the DIA online system data base and functional conversion of the DIAOLS programs/products) and to define the corresponding design approach which implements these requirements. Existing programs/products and data will be analyzed to verify that they are appropriately described in the Conversion Requirements Specification (CRS). The CRS has been baselined. A conversion plan will now be developed to identify all necessary conversion software.

The relationship between this task and the software evaluation and architecture subtasks is significant in that the selection of software packages can impact the conversion approach and the amount of conversion that must be performed for the DIA system. Also, the relationship between this task and the user language task is crucial because a large amount of the conversion activities will of necessity be performed by means of command procedures.

G. Systems Engineering Analysis

This effort will identify critical design areas which need to be addressed by the overall design and establish the system level architecture based on the software evaluation studies and resolution of the critical design issues. It will define the hardware architecture and establish design concepts for all external and device interfaces. Then the task will validate the overall design to ensure that the requirements are covered, the design is end-to-end complete, and that potential performance problems are identified and resolved. It will also coordinate the documentation of the design in the System Design Document (SDD) and coordinate the preparation and conduct of the System Design Review. A preliminary system test plan will also be developed to identify the integration and test approach which will be used for the Integrated Capabilities.

A preliminary list of critical design areas has been formulated. TRW personnel attended discussions on AIM with ODP and CSPO to learn more of current system architecture. The current architecture for systems that will form a part of the SAFE early capability system as well as other similar packages currently operational within the ODP computing center is being analyzed. Information received to date on the architectures of AIM, PMO, TADS and CAMS II revealed several problems which need resolution in order that the SAFE system can serve a larger user community. An improved message dissemination algorithm for PMO is being developed. It shall be evaluated for incorporation into the SAFE design. A preliminary paper has been prepared which

focuses on the architectural questions that need further investigation as potential enhancements, alternatives, or design changes to serve the larger user population are considered.

It is clear that there is a wide range of possible architectures to pursue. Some major architecture issues will be ordered in priority to reduce the range of alternatives. The software evaluation criteria will be reviewed with respect to potential architectural environments in which the software may reside. A list of critical system design issues will be published to coordinate the system design activity.

It is still deemed correct to have the user interactive environment supported by the VM operating system and the message analysis/dissemination and DBMS support to be hosted under the MVS operating system. Aspects of the AIM package modifications for the CAMS II project appear applicable to SAFE for supporting the user interface.

VI. SCHEDULE

The development schedule has been divided into several phases. The first phase is for study prior to the generation of a system design. It is called the evaluation phase. During this period, July - Sept. 1982; software packages for use in the SAFE are being identified as well as the augmentations to them required to achieve the needed functions. The phasing of the functional deliveries as integrated capabilities will also be determined.

Table VII illustrates the proposed scheduling of the Evaluation Phase tasks and the following system design phase, Sept 1982 - Jan 1983. During this period, the system design will be generated based on the results of the study during the evaluation phase. A project plan will be developed by November 1982. It will contain detailed costs and schedules for the project. A formal presentation of the design, costs, and schedules will occur in February 1983 at the System Design Review. At present, four deliveries of integrated capabilities are proposed. They are discussed below and shown in relationship to the above mentioned activities in Table VIII.

Occurring simultaneously with the evaluation phase is planning for an Early Capability. This capability is off-the-shelf with very little development. It primarily provides expanded user access to the currently installed Pilot Mail Operation (PMO) for the CIA. The number of users will be increased from 45 to 300; 150 users will be able to access the system simultaneously. PMO, developed by Chase, Rosen, and Wallace, Inc. (CRW), draws upon capabilities of Interim SAFE. It provides a partial version of the mail operation intended for SAFE. PMO, in conjunction with ODP's Automated Information Management (AIM) software package, will provide both mail support functions and electronic mail (message routing). The AIM software is support in the VM/CMS operating system. This operating system provides text editing, text composition, and file handling services. PMO runs under the MVS operating system. All this software operates on IBM-compatible hardware. CIA message traffic to this system will be provided from the CIA Communications Center. All CIA terminals will have the capability of accessing the Ruffing Computer Center. COMTEN communications switching hardware will be used to achieve this capability. A duplicate of this service will be provided to DIA. Until the new DIA building is ready for equipment installation, the DIA capability will be housed in the CIA SAFE Computer Center, but separate from the CIA machines. Access to the DIA message traffic will be provided by providing telecommunications lines from the Pentagon. Terminal access will be from Arlington Hall Station, Pentagon and Pompino Plaza. A third facility to be housed in the CIA Computer Center, during this phase, is an unclassified (and therefore separate)

TASK SUMMARY SCHEDULE



~~SECRET~~

Table VII (continued)

Approved For Release 2006/08/17 : CIA-RDP83M00914R002000190004-0

TASK SUMMARY SCHEDULE (Continued)

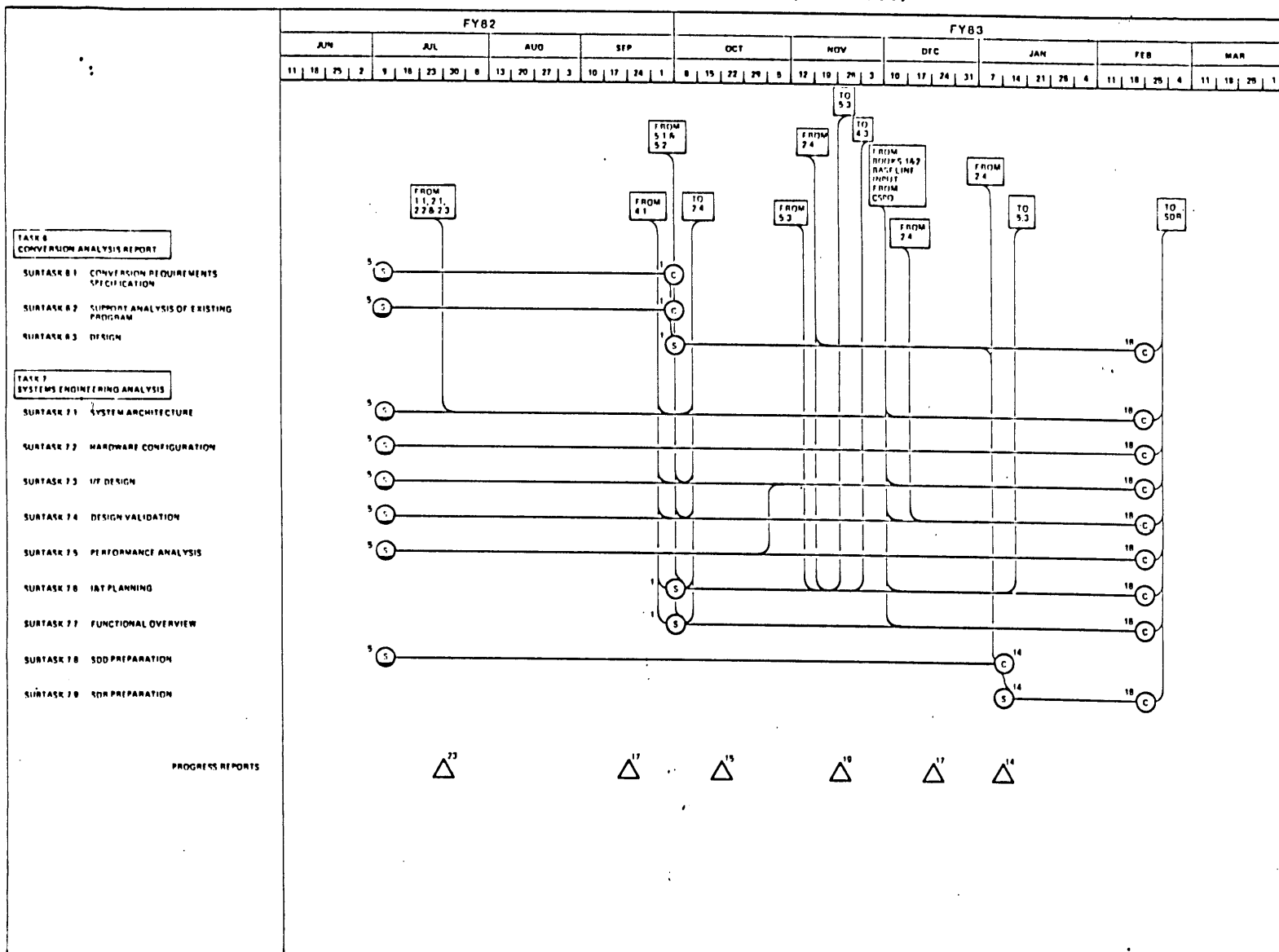
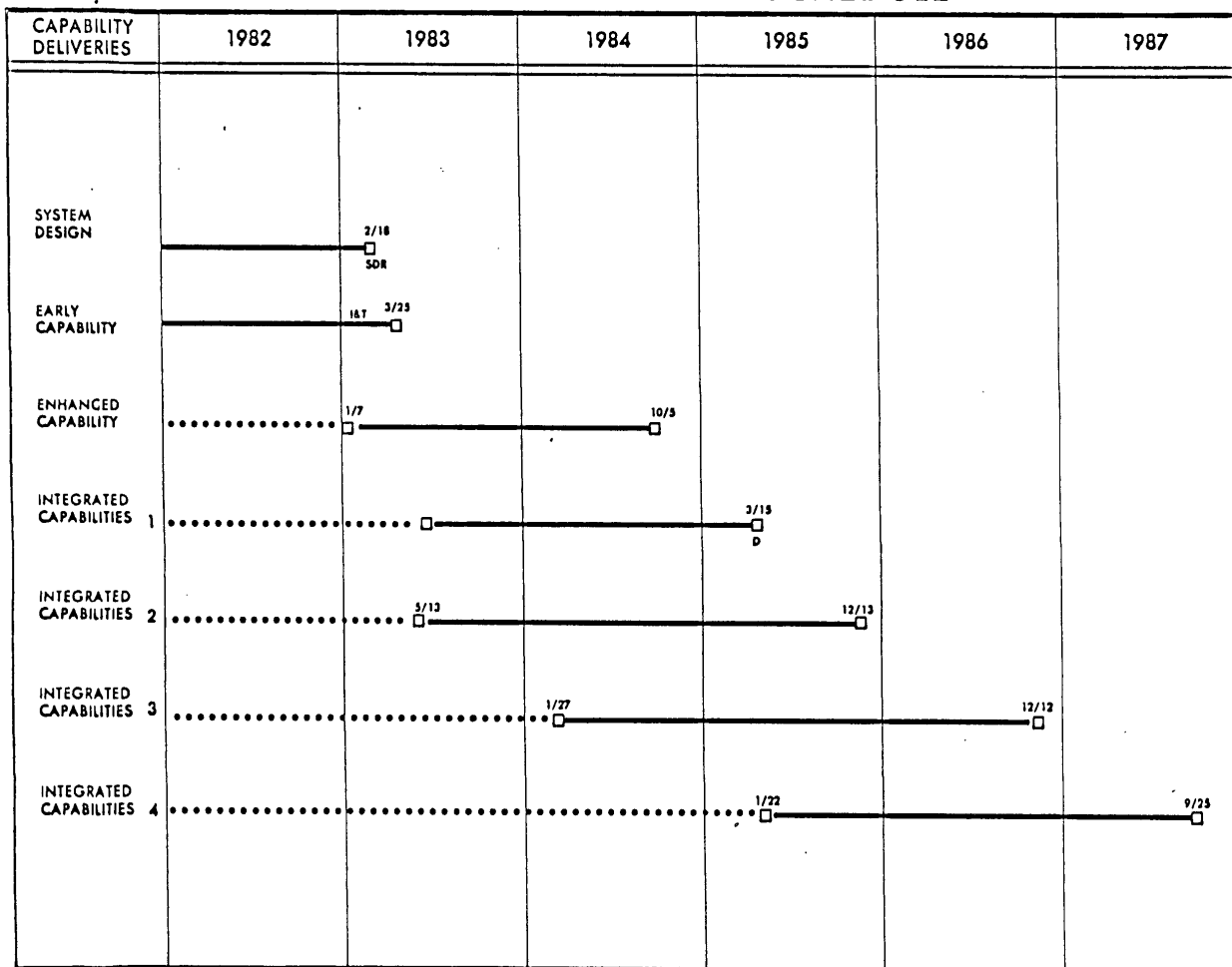


Table VII

IBM DEVELOPMENT SCHEDULE



..... CONCURRENCY

development system for the Integrated Capability.

The project plan for the Early Capability will be completed by late September 1982. A detailed design review is scheduled for early October 1982. The Early Capability will be operational in March 1983 for CIA and in May 1983 for DIA.

An Enhanced Capability is scheduled to be operational by October 1984. This has been viewed as a follow-on to the Early Capability in which the PMO and AIM software is augmented. Specific enhancements include: the on-line text search software (COLTS), from Interim SAFE, is moved from the MVS operating system to the VM/CMS operating system, an enhanced word processing capability is provided, a prototype of the SAFE User Language interface is provided, PMO is integrated with AIM under the VM operating system, an improved message dissemination algorithm is provided, and the number of users is expanded to 500 user (with 250 concurrent) in both the CIA and DIA systems.

Integrated Capability One is scheduled for March 1985. In this delivery, an inverted index search for structured data is provided. Enhanced mail analysis algorithms are available. Conversion of the CIA's central index (RECON) is provided as well as the initiation of conversion for the DIA's structured file environment (specifically the AIF, DIOBS, and Crisis Management File Systems will have begun). An initial integrated user interface is provided.

Integrated Capability Two is scheduled for December 1985. This will include combined text searching and structured file searching for mail as well as inverted text file searching for retrospective intelligence analysis activities. The number of users supported is expanded to 1000 for each Agency. Conversion of the installation files and order of battle files will be completed.

In Integrated Capability Three, scheduled for December 1986, additional functions and modifications to the previous capabilities are provided. Conversion of the DIA files continues with incorporation of the CRD, HUMINT, and SIGINT file systems. User experience with the previous deliveries will generate new requirements which shall be reflected in this and subsequent deliveries.

With the delivery of Integrated Capability Four, in September 1987, it is expected that all SAFE capability previously contracted for will have been provided. SAFE development should subsequently reflect normal system operations and maintenance activity. The level of this activity will be directly related to changes in the missions and functions of the user organizations.

The SAFE ongoing initiative will show [REDACTED] 45X1
[REDACTED] DIA) in FY 1988 (in then-year dollars). This includes 65X1
for an additional CPU mainframe for each agency as
well as normal hardware and software maintenance costs and some
applications software development.

VII. Costs

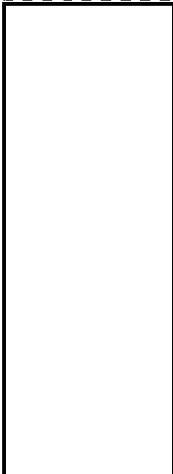
The costs for FY83-FY87 (in 1982 dollars) to complete the project using the software development approach (Burroughs) were estimated to be [REDACTED] 25X1 using the software integration (IBM or compatible) approach. The software development approach requires higher expenditure for software implementation than hardware procurement while the software integration approach requires higher expenditure for the hardware purchases. Although the [REDACTED] was based on 25X1 CSPO and TRW's best estimate based on their previous involvement and understanding of the Burrough's environment, chances for achieving a successful SAFE system through a major software development was considered very high risk and even if successful, would represent a one of a kind system not readily compatible with the ADP environment within CIA and DIA/DODIIS.

Table IX is a breakout of costs for the software integration approach to SAFE. Emphasis is on reducing costs associated with major software development and shifting those costs into hardware procurement. Under the previous approach to SAFE implementation (major software development) software costs were more than double the [REDACTED] and hardware costs were less than half the [REDACTED] 25X1 25X1

Table X provides funding profiles by Agency with cost shown in then-year escalated dollars to include personnel costs and will be reflected in the FY84 program submissions.

Table IX

COST/FUNDING BREAKOUT
(IN MILLIONS OF 1982 DOLLARS)
FY-1983 to FY-1987
SOFTWARE INTEGRATION OPTION (BUY/PURCHASE PLAN)

	Total	
SOFTWARE		25X1
CONVERSION		
COMMUNICATIONS		
HARDWARE		
- COMPUTER EQUIP		
- TERMINALS		
- PRINTERS		
ADMINISTRATIVE		
- DEV FACILITY		
- RELOCATION		
- CONTRACTOR TRAVEL		
- STAFF TRAVEL		

*SOFTWARE DEVELOPMENT UNCERTAINTY MAY ADD UP TO  POSSIBLY
OFFSET BY BETTER NEGOTIATED PRICES ON HARDWARE, INCLUDED HERE AT
LIST PRICE

25X1

Page Denied